

**UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE**

BERNADETTE HIGHTOWER, LATERSHIA  
JONES, and GEORGE DEAN, individually and  
on behalf of all others similarly situated,

Plaintiffs,

v.

RECEIVABLES PERFORMANCE  
MANAGEMENT, LLC,

Defendant.

Lead Case No. 2:22-cv-01683-RSM

**CONSOLIDATED CLASS ACTION  
COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiffs Bernadette Hightower, Latershia Jones, and George Dean (collectively, “Plaintiffs”), individually and on behalf of all others similarly situated, and by and through their undersigned counsel, file this Consolidated Class Action Complaint against Defendant Receivables Performance Management, LLC (“RPM” or “Defendant”) and allege the following based upon personal knowledge of the facts, and upon information and belief based on the investigation of counsel as to all other matters.

**NATURE OF THE ACTION**

1. Defendant provides debt collection services to various businesses, including telecommunications providers, utility providers, and financial institutions. To provide these services and in the ordinary course of RPM’s business, Defendant acquires, processes, analyzes,

1 and otherwise utilizes the personally identifiable information of purported debtors, including, but  
2 not limited to, their names and Social Security numbers (“PII”).

3 2. Defendant owed common law, contractual, and statutory duties to Plaintiffs and  
4 Class Members to design and implement adequate data security systems to protect the PII in its  
5 possession.

6 3. Moreover, by taking possession and control of Plaintiffs’ and Class Members’ PII,  
7 and utilizing the PII for its business purposes, Defendant assumed a duty to securely store and  
8 protect that sensitive information.

9 4. Defendant breached these duties by failing to properly safeguard and protect  
10 Plaintiffs’ and Class Members’ PII from a foreseeable cyberattack on its systems.

11 5. Specifically, on or about April 8, 2021, cybercriminals targeted, accessed,  
12 exfiltrated, and stole files on Defendant’s network containing the PII of Plaintiffs and millions of  
13 other Class Members (the “Data Breach”). Defendant’s monitoring practices were so poor that it  
14 did not identify this intrusion until May 12, 2021. Then, RPM reprehensibly waited until  
15 November 21, 2022—more than a year later—to begin notifying victims of the Data Breach.

16 6. Defendant has disclosed that in total, the Data Breach compromised the PII of  
17 approximately 3,766,573 people, including Plaintiffs’ and Class Members’ names and Social  
18 Security numbers.<sup>1</sup>

19 7. Defendant’s negligent conduct—including, but not limited to, failing to implement  
20 adequate and reasonable data security measures to protect Plaintiffs’ and Class Members’ PII;  
21 failing to timely detect the Data Breach; failing to take adequate steps to prevent and stop the Data  
22 Breach; failing to disclose the material facts that it did not have adequate security practices and  
23 employee training in place to safeguard the PII; failing to honor its promises and representations  
24

---

25 <sup>1</sup>See Office of the Maine Attorney General, [https://apps.web.maine.gov/online/aeviewer/](https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml)  
26 ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml (posting of data breach) (last visited Feb.  
16, 2023).

1 to protect Plaintiffs' and Class Members' PII; and failing to provide timely and adequate notice of  
2 the Data Breach—caused substantial harm and injuries to Plaintiffs and Class Members across the  
3 United States.

4 8. Furthermore, due to Defendant's negligence and data security failures,  
5 cybercriminals accessed, exfiltrated, and now likely possess, every type of PII they need to commit  
6 identity theft and wreak havoc on the financial and personal lives of millions of individuals.

7 9. As a result of the Data Breach, Plaintiffs and Class Members have suffered actual  
8 damages from the invasion of their privacy. Moreover, as a result of Plaintiffs' PII has been  
9 released to cybercriminals, Plaintiffs and Class Members are at an imminent, impending, and  
10 current risk of identity theft and fraud. This risk is realized and will continue for the rest of their  
11 lives, as Plaintiffs and Class Members are now forced to deal with the danger of identity thieves  
12 possessing and fraudulently using their PII.

13 10. In response to the Data Breach, Plaintiffs and Class Members lost time and money  
14 attempting to mitigate the impact of the Data Breach and following Defendant's warnings.  
15 Plaintiffs and Class Members anticipate spending additional time and money further mitigating  
16 the impact of the Data Breach, including but not limited to the cost of future identity theft  
17 monitoring services.

18 11. To be sure, the risk of harm is imminent and concrete, as Plaintiff Hightower  
19 suffered actual fraudulent activity in her bank accounts, and Plaintiffs Jones and Dean both  
20 suffered a misuse of their data with the publication of their PII on the dark web. Other Class  
21 Members are believed to have experienced and suffered the same damages and losses throughout  
22 the country.

23 12. Plaintiffs brings this action individually and on behalf of the Class and seek past  
24 and future compensatory damages, nominal damages, statutory damages, treble damages,  
25 restitution, and injunctive and declaratory relief (including significant improvements to  
26 Defendant's data security protocols and employee training practices), reasonable attorney's fees,

1 costs, and expenses incurred in bringing this action, and all other remedies this Court deems just  
2 and proper.

3 **THE PARTIES**

4 13. Plaintiff Hightower is, and at all relevant times has been, a resident and citizen of  
5 the State of Pennsylvania.

6 14. Plaintiff Latershia Jones is, and at all relevant times has been, a citizen and resident  
7 of the Commonwealth of Virginia.

8 15. Plaintiff Dean is, and at all relevant times has been, a resident and citizen of the  
9 State of Georgia.

10 16. Defendant is a Washington limited liability company with its principal place of  
11 business at 20818 44th Ave. W., Ste. 240, Lynnwood, WA 98036.

12 **JURISDICTION AND VENUE**

13 17. This Court has diversity jurisdiction over this action under the Class Action  
14 Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100  
15 Class Members, the amount in controversy exceeds \$5,000,000, exclusive of interest and costs,  
16 and Plaintiffs and members of the Class are citizens of states that differ from Defendant.

17 18. This Court has personal and general jurisdiction over Defendant because  
18 Defendant's principal place of business is located in this District, and Defendant conducts  
19 substantial business in Washington and this District through its principal place of business.

20 19. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391  
21 because Defendant is headquartered in this District and a substantial part of the events or omissions  
22 giving rise to Plaintiffs' claims occurred in this District.

23 **FACTUAL ALLEGATIONS**

24 **A. The Data Breach**

25 20. For RPM to perform its debt collection services, from which it generates its profits,  
26 Defendant collects and stores the PII of individuals, including Plaintiffs and the Class.

1           21. Due to the highly sensitive and personal nature of the information Defendant  
2 acquires and stores with respect to purported debtors, Defendant recognizes the privacy rights of  
3 the individuals whose PII Defendant obtains, as evidenced by RPM's publicly available privacy  
4 policy ("Privacy Notice").<sup>2</sup> Through its Privacy Notice, Defendant promises to maintain the  
5 privacy of individuals' PII and not disclose their PII without authorization. In particular, the  
6 Privacy Notice assures:

7           We recognize and respect the privacy expectations of all people and make the  
8 safekeeping of all information a priority. . . . Our employees are educated on the  
9 importance of maintaining the confidentiality of information and of our privacy  
10 policy. In the event of a privacy breach by an employee, appropriate disciplinary  
11 action will be taken. ***We will maintain physical, electronic and procedural  
safeguards to guard against unauthorized access to information.***

12           (emphasis added).

13           22. Plaintiffs and Class Members reasonably expected that Defendant would  
14 implement and maintain reasonable data security measures to protect their PII from foreseeable  
15 cybersecurity threats.

16           23. On or about May 12, 2021, Defendant became aware of a data security incident that  
17 impacted its server infrastructure and subsequently took Defendant's system offline. Defendant  
18 retained a forensic investigation firm that determined Defendant's systems were first accessed by  
19 cybercriminals on or about April 8, 2021. During this time, cybercriminals "accessed or acquired"  
20 Plaintiffs' and Class Members' PII, including their Social Security numbers. More than 3,700,000  
21 victims had their PII exposed as a result of the Data Breach.<sup>3</sup>

22           24. Based on Defendant's acknowledgement that PII was "acquired" by  
23

---

24           <sup>2</sup> RPM, Receivables Performance Management, LLC,  
25 <http://www.receivablesperformance.com/PrivacyPolicy.aspx> (last visited Feb.16, 2023).

26           <sup>3</sup> Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml> (posting of data breach) (last visited Feb. 16, 2023).

1 cybercriminals, it is evident that unauthorized cybercriminals did in fact access Defendant's files,  
2 and then exfiltrated and stole Plaintiffs' and Class Members' PII from those files.

3 25. On information and belief, Defendant failed to encrypt the PII contained in the files  
4 accessed by cybercriminals.

5 26. On information and belief, the cyberattack was targeted at Defendant due to its  
6 status as a major debt collector that obtains and stores large amounts of PII.

7 27. On information and belief, the targeted attack was expressly designed to gain access  
8 to and exfiltrate and steal private and confidential data, including the PII of Plaintiffs and the Class  
9 Members for criminal misuse, e.g., identity theft and financial fraud.

10 28. Moreover, while Defendant admits it learned of the Data Breach in May 2021,  
11 Defendant inexplicably waited *one year and six months* before it began the process of notifying  
12 impacted individuals, such as Plaintiffs and Class Members.

13 29. The fact that Defendant needed more than eighteen (18) months after learning of  
14 the Data Breach to investigate and begin notifying the impacted individuals of the need for them  
15 to protect themselves against fraud and identity theft only highlights the very poor state of  
16 Defendant's data security and tracking systems. Defendant was, of course, too late in the  
17 discovery, investigation, and notification of the Data Breach, which further left Plaintiff and Class  
18 Members' PII exposed.

19 30. Due to Defendant's inadequate security measures and its delayed notice to victims,  
20 Plaintiffs and the Class Members now face a present, immediate, and ongoing risk of fraud and  
21 identity theft and must deal with that threat forever.

22 31. Defendant had duties and obligations created by industry standards, common law,  
23 and its own promises and representations made to Plaintiffs and Class Members to keep their PII  
24 confidential and to protect that PII from unauthorized access and disclosure.

25 32. Plaintiffs and Class Members had the reasonable expectation that Defendant would  
26 comply with its duties and obligations to keep such information confidential and secure from

1 unauthorized access and theft.

2 33. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs’  
3 and Class Members’ PII, Defendant assumed legal and equitable duties and knew or should have  
4 known that it was responsible for protecting Plaintiffs’ and Class Members’ PII from unauthorized  
5 disclosure.

6 34. As a result of Defendant’s negligent and wrongful conduct, Plaintiffs’ and Class  
7 Members’ sensitive PII was maintained in an inadequate and unsafe condition that allowed  
8 foreseeable criminal actors to access, exfiltrate, and steal their PII causing past, present, and future  
9 harms.

## 10 **B. Plaintiffs’ Experiences**

### 11 *Plaintiff Hightower’s Experience*

12 35. Plaintiff Hightower greatly values her privacy and is very careful with her PII.  
13 Plaintiff Hightower stores any documents containing PII in a safe and secure location or destroys  
14 such documents when they are no longer needed. Plaintiff Hightower has never knowingly  
15 transmitted sensitive PII over the internet in a manner that is unencrypted or unsecured. Moreover,  
16 Plaintiff Hightower diligently chooses unique usernames and passwords for her various online  
17 accounts. When Plaintiff Hightower does entrust a third-party with her PII, it is only because she  
18 understands such information will be reasonably safeguarded from foreseeable threats, and that  
19 she will be timely notified if her data is exposed.

20 36. Plaintiff Hightower provided PII, including her name, date of birth, and Social  
21 Security number, to her credit card company, one of Defendant’s accounts receivable management  
22 clients, as a condition of receiving financial services. Upon information and belief, Defendant  
23 thereafter acquired this PII and used this information when attempting to collect a purported debt.

24 37. Plaintiff Hightower received a letter dated November 21, 2022, from Defendant  
25 notifying her of the Data Breach. The letter advised that unauthorized third parties had accessed  
26 and exfiltrated files on Defendant’s server containing Plaintiff Hightower’s “personal information

1 . . . including Social Security number . . . .”

2 38. Recognizing the present, immediate, and substantial risk of identity theft and fraud  
3 that Plaintiff Hightower now faces, Defendant offered Plaintiff Hightower a twelve-month  
4 subscription to credit monitoring services, which Defendant advised Plaintiff Hightower to enroll  
5 in so that she can “protect” herself “from potential harm associated with this incident . . . .” The  
6 letter further cautioned and warned Plaintiff Hightower to “remain vigilant for incidents of fraud  
7 and identity theft by reviewing account statements, explanation of benefit statements, and credit  
8 reports for unauthorized activity . . . .”

9 39. As a result of the Data Breach, Plaintiff Hightower heeded Defendant’s warnings  
10 and advice and has spent approximately 30 hours researching the Data Breach, verifying the  
11 legitimacy of the notice letter, reviewing her bank accounts, monitoring her credit report, working  
12 with her financial institutions, filing a police report, changing her passwords and payment account  
13 numbers, and taking other necessary mitigation efforts. This is valuable time Plaintiff Hightower  
14 has spent at Defendant’s direction and in response to the Data Breach that she otherwise would  
15 have spent on other activities, including but not limited to work and/or recreation.

16 40. In addition, as a result of the Data Breach, Plaintiff Hightower suffered actual fraud  
17 with fraudulent activity on her Citizens Bank account in the early Summer of 2022 and more  
18 recently in October 2022. Specifically, Plaintiff Hightower noticed small amounts of money  
19 withdrawn from her bank account without her authorization.

20 41. Plaintiff Hightower would not have allowed her PII to be maintained by RPM had  
21 she known that Defendant would fail to safeguard that information from unauthorized access.

22 42. The Data Breach and fraudulent use of her PII also directly caused Plaintiff  
23 Hightower to suffer a loss of privacy.

24 43. As a result of the Data Breach, Plaintiff Hightower faces a substantial and imminent  
25 threat of identity theft and fraud that will exist for the rest of her life.

26 44. In response to the Data Breach and in heeding Defendant’s warnings, Plaintiff



1 Hightower has spent and anticipates spending additional time and money on an ongoing basis to  
 2 try to mitigate and address the present and impending harm caused by the Data Breach.

3 45. The invasion of privacy and the substantial risk of identity theft and fraud have each  
 4 caused Plaintiff Hightower to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

5 46. The Data Breach further caused Plaintiff Hightower to suffer a diminution in the  
 6 value of her PII.

7 47. Plaintiff Hightower has a continuing interest in ensuring that her PII, which upon  
 8 information and belief, remains in Defendant's possession, is protected, and safeguarded from  
 9 future breaches.

10 ***Plaintiff Jones' Experience***

11 48. Plaintiff Jones greatly values her privacy and is very careful with her PII. Plaintiff  
 12 Jones stores any documents containing PII in a safe and secure location or destroys such documents  
 13 when they are no longer needed. Plaintiff Jones has never knowingly transmitted sensitive PII over  
 14 the internet in a manner that is unencrypted or unsecured. Moreover, Plaintiff Jones diligently  
 15 chooses unique usernames and passwords for her various online accounts. When Plaintiff Jones  
 16 does entrust a third-party with her PII, it is only because she understands such information will be  
 17 reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is  
 18 exposed.

19 49. Plaintiff Jones provided PII, including her name, date of birth, and Social Security  
 20 number, to one of Defendant's clients as a condition of receiving services. Upon information and  
 21 belief, Defendant thereafter acquired this PII and used this information when attempting to collect  
 22 a purported debt.

23 50. Plaintiff Jones received a letter dated November 21, 2022, from Defendant  
 24 notifying her of the Data Breach. The letter indicated that unauthorized third parties accessed and  
 25 exfiltrated files on Defendant's server containing Plaintiff Jones's "personal information . . .  
 26 including Social Security number . . . ."

1           51. Recognizing the present, immediate, and substantial risk of identity theft and  
2 imminent financial harm that Plaintiff Jones now faces, Defendant offered Plaintiff Jones a twelve-  
3 month subscription to credit monitoring services, which Defendant encouraged Plaintiff Jones to  
4 enroll in so that she can “protect” herself “from potential harm associated with this incident . . . .”  
5 The letter further cautioned and warned Plaintiff Jones to “remain vigilant for incidents of fraud  
6 and identity theft by reviewing account statements, explanation of benefit statements, and credit  
7 reports for unauthorized activity ....”

8           52. As a result of the Data Breach, Plaintiff Jones heeded Defendant’s warning and has  
9 spent numerous hours researching the Data Breach, verifying the legitimacy of the notice letter,  
10 placing freezes on her credit, reviewing her bank accounts, monitoring her credit reports,  
11 monitoring her other information, changing her passwords and other identifying information, and  
12 taking other necessary mitigation efforts. This is valuable time Plaintiff Jones spent at Defendant’s  
13 direction and that she otherwise would have spent on other activities, including but not limited to  
14 work and/or recreation.

15           53. In addition, Plaintiff Jones has already experienced data misuse as a result of the  
16 Data Breach. Specifically, in the months following the Data Breach, Plaintiff Jones received  
17 notification that her Social Security number was compromised and found on the dark web.

18           54. Plaintiff Jones would not have allowed her PII to be maintained by RPM had she  
19 known that Defendant would fail to safeguard that information from unauthorized access.

20           55. The Data Breach and publication of her information on the Dark Web has caused  
21 Plaintiff Jones to suffer a loss of privacy.

22           56. As a result of the Data Breach, Plaintiff Jones faces a substantial and imminent  
23 threat of identity theft and fraud that she will face for the remainder of her life.

24           57. Plaintiff Jones has spent time and anticipates spending considerable time and  
25 money on an ongoing basis to try to mitigate and address the present and impending injuries caused  
26 by the Data Breach.

1           58.     The invasion of privacy and substantial risk of identity theft and fraud have each  
2 caused Plaintiff Jones to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

3           59.     The Data Breach caused Plaintiff Jones to suffer a diminution in the value of her  
4 PII.

5           60.     Plaintiff Jones has a continuing interest in ensuring that her PII, which upon  
6 information and belief, remains in Defendant's possession, is protected, and safeguarded from  
7 future breaches.

8                   ***Plaintiff Dean's Experience***

9           61.     Plaintiff Dean greatly values his privacy and is very careful with his PII. Plaintiff  
10 Dean stores any documents containing PII in a safe and secure location or destroys such documents  
11 when they are no longer needed. Plaintiff Dean has never knowingly transmitted sensitive PII over  
12 the internet in any manner that is unencrypted or unsecured. Moreover, Plaintiff Dean diligently  
13 chooses unique usernames and passwords for his online accounts. When Plaintiff Dean does  
14 entrust a third-party with his PII, it is only because he understands such information will be  
15 reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is  
16 exposed.

17           62.     Plaintiff Dean provided PII, including his name, date of birth, and Social Security  
18 number, to one of Defendant's clients as a condition of receiving services. Upon information and  
19 belief, Defendant thereafter acquired this PII and used this information when attempting to collect  
20 a purported debt.

21           63.     Plaintiff Dean received a letter dated November 21, 2022, from Defendant notifying  
22 him of the Data Breach. The letter advised that unauthorized third parties accessed and exfiltrated  
23 files on Defendant's server containing Plaintiff Dean's "personal information . . . including Social  
24 Security number . . . ."

25           64.     Recognizing the present, immediate, and substantial risk of identity theft and  
26 imminent financial harm Plaintiff Dean faces, Defendant offered Plaintiff Dean a twelve-month

1 subscription to credit monitoring services, which Defendant encouraged Plaintiff Dean to enroll in  
2 so that he can “protect” himself “from potential harm associated with this incident . . . .” The letter,  
3 however, did not include any instructions on how to enroll in the service.

4 65. Defendant further cautioned and warned Plaintiff Dean to “remain vigilant for  
5 incidents of fraud and identity theft by reviewing account statements, explanation of benefits  
6 statements, and credit reports for unauthorized activity . . . .”

7 66. Additionally, on January 25, 2023, Plaintiff Dean received a notification from  
8 IDNotify that his personal information was found on the Dark Web.

9 67. As a result of the Data Breach, and in heeding Defendant’s warnings, Plaintiff Dean  
10 spent more than five (5) hours researching the Data Breach, verifying the legitimacy of the notice  
11 letter, reviewing his bank accounts, monitoring his credit report, changing passwords, and other  
12 necessary mitigation efforts. This is valuable time Plaintiff Dean spent at Defendant’s direction  
13 and that he otherwise would have spent on other activities, including but not limited to work and/or  
14 recreation.

15 68. Plaintiff Dean would not have allowed his PII to be maintained by RPM had he  
16 known that Defendant would fail to safeguard that information from unauthorized access.

17 69. The Data Breach and subsequent publication of his PII on the dark web caused  
18 Plaintiff Dean to suffer a loss of privacy.

19 70. As a result of the Data Breach, Plaintiff Dean now faces a substantial risk of identity  
20 theft and imminent financial harm for the remainder of his life.

21 71. Plaintiff Dean has spent considerable time and anticipates spending considerable  
22 time and money on an ongoing basis to try to mitigate and address the present and impending harm  
23 caused by the Data Breach.

24 72. The invasion of privacy and substantial risk of identity theft and fraud have each  
25 caused Plaintiff Dean to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

26 73. The Data Breach caused Plaintiff Dean to suffer a diminution in the value of his

1 PII.

2 74. Plaintiff Dean has a continuing interest in ensuring that his PII, which upon  
3 information and belief, remains in Defendant's possession, is protected, and safeguarded from  
4 future breaches.

5 **C. Defendant Was on Notice of Data Threats in the Industry and of the Inadequacy**  
6 **of Its Data Security**

7 75. Defendant was on notice that companies, such as Defendant, maintaining large  
8 amounts of PII during their regular course of business, are prime targets for criminals looking to  
9 gain unauthorized access to sensitive and valuable information, such as the type of data at issue in  
10 this matter.

11 76. At all relevant times, RPM knew, or should have known, that the PII that it collected  
12 was a target for malicious actors. Despite such knowledge, and well-publicized cyberattacks on  
13 similar companies, RPM failed to implement and maintain reasonable and appropriate data privacy  
14 and security measures to protect Plaintiffs' and Class Members' PII from cyber-attacks that RPM  
15 should have anticipated and guarded against.

16 77. It is well known among companies that store sensitive PII that sensitive  
17 information—such as the Social Security numbers stolen in the Data Breach—is valuable and  
18 frequently targeted by criminals. In a recent article, *Business Insider* noted that “[d]ata breaches  
19 are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by  
20 flaws in . . . systems either online or in stores.”<sup>4</sup>

21 78. In light of recent high profile data breaches, including Microsoft (250 million  
22 records, December 2019), T-Mobile (110 million records, August 2021), Wattpad (268 million  
23 records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records,

---

24 <sup>4</sup> Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19*  
25 *companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05  
26 A.M.), <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>  
(last visited Feb. 16, 2023).

January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), RPM knew or should have known that its electronic records would be targeted by cybercriminals.

79. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

80. Moreover, PII is a valuable property right.<sup>5</sup> “Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks.”<sup>6</sup> American companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in 2018.<sup>7</sup> It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the “cyber black-market” or the “dark web” for many years.

81. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

82. Consumers place a high value on the privacy of that data, as they should.

---

<sup>5</sup> See Marc van Lieshout, *The Value of Personal Data*, 457 INT’L FED’N FOR INFO. PROCESSING 26 (May 2015) (“The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . .”), [https://www.researchgate.net/publication/283668023\\_The\\_Value\\_of\\_Personal\\_Data](https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data).

<sup>6</sup> OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220, Apr. 2, 2013, <https://doi.org/10.1787/5k486qtxldmq-en>.

<sup>7</sup> IAB Data Center of Excellence, *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/>.

1 Researchers shed light on how much consumers value their data privacy—and the amount is  
 2 considerable. Indeed, studies confirm that “when privacy information is made more salient and  
 3 accessible, some consumers are willing to pay a premium to purchase from privacy protective  
 4 websites.”<sup>8</sup>

5 83. Given these facts, any company that transacts business with a consumer and then  
 6 compromises the privacy of consumers’ PII has thus deprived that consumer of the full monetary  
 7 value of the consumer’s transaction with the company.

#### 8 **D. Cyber Criminals Will Use Plaintiffs’ and Class Members’ PII to Defraud Them**

9 84. Plaintiffs’ and Class Members’ PII is of great value to cyber criminals, and the data  
 10 stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways  
 11 for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

12 85. Each year, identity theft causes tens of billions of dollars of losses to victims in the  
 13 United States.<sup>9</sup> For example, with the PII stolen in the Data Breach, which includes Social Security  
 14 numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns,  
 15 commit crimes, create false driver’s licenses and other forms of identification and sell them to  
 16 other criminals or undocumented immigrants, steal government benefits, give breach victims’  
 17 names to police during arrests, and many other harmful forms of identity theft.<sup>10</sup> These criminal  
 18 activities have and will result in devastating financial and personal losses to Plaintiffs and Class  
 19 Members.

---

21 <sup>8</sup> Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*,  
 22 *An Experimental Study*, 22(2) INFO. SYS. RES. 254 (June 2011)  
<https://www.jstor.org/stable/23015560?seq=1>.

23 <sup>9</sup> “Facts + Statistics: Identity Theft and Cybercrime,” INS. INFO. INST.,  
 24 <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing Javelin  
 Strategy & Research’s report “2018 Identity Fraud: Fraud Enters a New Era of Complexity”) (last accessed Feb. 16, 2023).

25 <sup>10</sup> See, e.g., Christine DiGangi, *What Can You Do with a Stolen Social Security Number?*,  
 26 CREDIT.COM (June 29, 2020), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/> (last visited Feb. 16, 2023).



1 86. PII is such a valuable commodity to identity thieves that once it has been  
2 compromised, criminals will use it and trade the information on the cyber black-market for years.<sup>11</sup>

3 87. For example, it is believed that certain highly sensitive personal information  
4 compromised in the 2017 Experian data breach was being used, three years later, by identity  
5 thieves to apply for COVID-19-related unemployment benefits.<sup>12</sup>

6 88. The PII exposed the Data Breach is valuable to identity thieves for use in the kinds  
7 of criminal activity described herein. These risks are both certainly impending and substantial. As  
8 the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they  
9 will use it.<sup>13</sup>

10 89. Cyber criminals may not use the information right away. According to the U.S.  
11 Government Accountability Office, which conducted a study regarding data breaches:

12 [I]n some cases, stolen data may be held for up to a year or more before being used  
13 to commit identity theft. Further, once stolen data have been sold or posted on the  
14 Web, fraudulent use of that information may continue for years. As a result, studies  
15 that attempt to measure the harm resulting from data breaches cannot necessarily  
16 rule out all future harm.<sup>14</sup>

17 90. For instance, with a stolen Social Security number, which is only one category of  
18 the PII compromised in the Data Breach, someone can open financial accounts, file fraudulent tax  
19 returns, commit crimes, and steal benefits.<sup>15</sup>

20 <sup>11</sup> United States Government Accountability Office, Report to Congressional Requesters,  
21 *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the*  
22 *Full Extent Is Unknown* (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>.

23 <sup>12</sup> See Jon Fingas, *Fraud Ring Uses Stolen Data to Scam Unemployment Insurance*  
24 *Programs*, ENGADGET (May 17, 2020, 1:46 PM), [https://www.engadget.com/stolen-data-used-](https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html)  
25 [for-unemployment-fraud-ring-174618050.html](https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html) (last accessed Feb. 16, 2023); see also Lily H.  
26 Newman, *The Nigerian Fraudsters Ripping Off the Unemployment System*, WIRED (May 19,  
2020, 7:00 AM), [https://www.wired.com/story/nigerian-scammers-unemployment-system-](https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/)  
[scattered-canary/](https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/) (last visited Feb. 16, 2023).

<sup>13</sup> Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER  
(May 24, 2017), [https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-](https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info)  
stolen-info (last accessed Feb. 16, 2023).

<sup>14</sup> *Data Breaches Are Frequent*, *supra* note 11.

<sup>15</sup> See, e.g., *What Can You Do with a Stolen Social Security Number?*, *supra* note 10.



1           91. Victims of the Data Breach, like Plaintiffs and other Class Members, must spend  
2 many hours and large amounts of money protecting themselves from the current and future  
3 negative impacts to their privacy and credit because of the Data Breach.<sup>16</sup>

4           92. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class  
5 have been placed at an imminent, immediate, and continuing risk of harm from fraud and identity  
6 theft. Plaintiffs and the Class must now take the time and effort (and spend the money) to mitigate  
7 the actual and potential impact of the Data Breach on their everyday lives, including purchasing  
8 identity theft and credit monitoring services every year for the rest of their lives, placing “freezes”  
9 and “alerts” with credit reporting agencies, contacting their financial institutions, closing or  
10 modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports,  
11 and other information for unauthorized activity for years to come.

12           93. Plaintiffs and the Class have suffered or will suffer actual harms for which they are  
13 entitled to compensation, including but not limited to the following:

- 14           a. Trespass, damage to, and theft of their personal property, including PII;
- 15           b. Improper disclosure of their PII;
- 16           c. The imminent and certainly impending injury flowing from actual and potential  
17           future fraud and identity theft posed by their PII being in the hands of criminals  
18           and having already been misused;
- 19           d. The imminent and certainly impending risk of having their confidential  
20           information used against them by spam callers to defraud them;
- 21           e. Damages flowing from Defendant’s untimely and inadequate notification of the  
22           Data Breach;

---

23  
24           <sup>16</sup> Identity Theft – A Recovery Plan, FED. TRADE COMM’N, (Sept. 2018),  
25 [https://www.bulkorder.ftc.gov/system/files/publications/501a\\_idt\\_a\\_recovery\\_plan\\_508.pdf](https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf) (last  
26 visited Feb. 16, 2016); *see also* Identity Theft – What to Know, What to Do, FED. TRADE  
COMM’N (Sept. 2018), [https://www.bulkorder.ftc.gov/system/files/publications/](https://www.bulkorder.ftc.gov/system/files/publications/677a_idt_what_to_know_wtd.pdf)  
677a\_idt\_what\_to\_know\_wtd.pdf.

- 1 f. Loss of privacy suffered as a result of the Data Breach;
- 2 g. Ascertainable losses in the form of out-of-pocket expenses and the value of their
- 3 time reasonably expended to remedy or mitigate the effects of the data breach;
- 4 h. Ascertainable losses in the form of deprivation of the value of individuals'
- 5 personal information for which there is a well-established and quantifiable
- 6 national and international market;
- 7 i. The loss of use of and access to their credit, accounts, and/or funds;
- 8 j. Damage to their credit due to fraudulent use of their PII; and
- 9 k. Increased cost of borrowing, insurance, deposits, and other items, which are
- 10 adversely affected by a reduced credit score.

11 94. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII,  
 12 which remains in the possession of Defendant, is protected from further public disclosure by the  
 13 implementation of better employee training and industry standard and statutorily-compliant  
 14 security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting  
 15 Plaintiffs' and Class Members' PII.

16 95. Plaintiffs and Class Members have been taking and will continue to take  
 17 appropriate steps to mitigate the risk of harm and damage that Defendant has caused them but,  
 18 given the kind of PII Defendant made so easily accessible to cyber criminals, they are certain to  
 19 incur additional damages. Because identity thieves already have their PII, Plaintiffs and Class  
 20 Members will need to have identity theft monitoring protection for the rest of their lives. Some  
 21 may even need to go through the long and arduous process of getting a new Social Security  
 22 number, with all the loss of credit and employment difficulties that come with this change.<sup>17</sup>

---

25 <sup>17</sup>*What Happens if I Change My Social Security Number?*, LEXINGTON LAW (Aug. 10,  
 26 2022), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html> (last visited Feb. 16, 2023).

1           96. To be sure, Plaintiffs should not be in the current compromised position with  
 2 respect to their identities and financial affairs, and Plaintiffs should not have been forced to take  
 3 time consuming and expensive mitigation measures to protect themselves from identity theft and  
 4 fraud. None of this should have happened because the Data Breach was entirely preventable.

5           **E. Defendant Could Have Prevented the Data Breach but Failed to Adequately**  
 6           **Protect Plaintiffs’ and Class Members’ PII**

7           97. Data disclosures and data breaches are preventable.<sup>18</sup> As Lucy Thompson wrote in  
 8 the Data Breach and Encryption Handbook, “In almost all cases, the data breaches that occurred  
 9 could have been prevented by proper planning and the correct design and implementation of  
 10 appropriate security solutions.”<sup>19</sup> She added that “[o]rganizations that collect, use, store, and share  
 11 sensitive personal data must accept responsibility for protecting the information and ensuring that  
 12 it is not compromised . . . .”<sup>20</sup>

13           98. “Most of the reported data breaches are a result of lax security and the failure to  
 14 create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information  
 15 security controls, including encryption, must be implemented and enforced in a rigorous and  
 16 disciplined manner so that a *data breach never occurs*.”<sup>21</sup>

17           99. Defendant obtained and stored Plaintiffs’ and Class Members’ PII—including, but  
 18 not limited to, their names Social Security numbers—and was entrusted with properly holding,  
 19 safeguarding, and protecting against unlawful disclosure of such PII.

20           100. Defendant breached duties owed to Plaintiffs and the Class as guardian of their PII.

21           101. Many failures laid the groundwork for the occurrence of the Data Breach, starting  
 22 with Defendant’s failure to incur the costs necessary to implement adequate and reasonable cyber  
 23

---

24           <sup>18</sup> Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,”  
 25 DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

26           <sup>19</sup> *Id.* at 17.

<sup>20</sup> *Id.* at 28.

<sup>21</sup> *Id.*

1 security training, procedures, and protocols that were necessary to protect Plaintiffs' and Class  
2 Members' PII.

3 102. Defendant maintained the PII in an objectively reckless manner, making the PII  
4 vulnerable to unauthorized disclosure.

5 103. Defendant knew, or reasonably should have known, of the importance of  
6 safeguarding PII and of the foreseeable consequences that would occur if Plaintiffs' and Class  
7 Members' PII was stolen, including the significant costs that would be placed on Plaintiffs and  
8 Class Members as a result of a breach.

9 104. The risk of improper disclosure of Plaintiffs' and Class Members' PII was a known  
10 risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure  
11 Plaintiffs' and Class Members' PII from that risk left the PII in a dangerous condition.

12 105. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i)  
13 intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures  
14 to ensure that the PII was protected against unauthorized intrusions; (ii) failing to disclose that it  
15 did not have adequately robust security protocols and training practices in place to adequately  
16 safeguard Plaintiffs' and Class Members' PII; (iii) failing to take standard and reasonably available  
17 steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for  
18 an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt  
19 and accurate notice of the Data Breach.

20 ***i. Defendant Could Have Prevented the Data Breach by Implementing***  
21 ***Widely Distributed Expert-Recommended Measures***

22 106. Defendant could have prevented this Data Breach by properly securing and  
23 encrypting the systems containing the PII of Plaintiffs and Class Members. Alternatively,  
24 Defendant could have destroyed the data, especially for individuals with whom it had not had a  
25 relationship for a period of time or for whom there was no reasonably anticipated future use.  
26

1           107. Defendant’s negligence in safeguarding the PII of Plaintiffs and Class Members is  
 2 exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect  
 3 and secure sensitive data they possess.

4           108. Despite the prevalence of public announcements of data breach and data security  
 5 compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class  
 6 Members.

7           109. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud  
 8 committed or attempted using the identifying information of another person without authority.”  
 9 The FTC describes “identifying information” as “any name or number that may be used, alone or  
 10 in conjunction with any other information, to identify a specific person,” including, among other  
 11 things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s  
 12 license or identification number, alien registration number, government passport number,  
 13 employer or taxpayer identification number.”<sup>22</sup>

14           110. The ramifications of Defendant’s failure to keep secure the PII of Plaintiffs and  
 15 Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information  
 16 and damage to victims may continue for years.

17           111. To prevent and detect unauthorized cyber-attacks, Defendant could and should  
 18 have implemented, as recommended by the United States Government, the following measures:

- 19           • Implement an awareness and training program. Because end users  
 20 are targets, employees and individuals should be aware of the threat  
 of ransomware and how it is delivered.
- 21           • Enable strong spam filters to prevent phishing emails from reaching  
 22 the end users and authenticate inbound email using technologies like  
 23 Sender Policy Framework (SPF), Domain Message Authentication  
 Reporting and Conformance (DMARC), and DomainKeys  
 24 Identified Mail (DKIM) to prevent email spoofing.

25 \_\_\_\_\_  
 26 <sup>22</sup> See generally <https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business> (last accessed October 21, 2022).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>23</sup>

112. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . . .
- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . . .
- Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it . . . .
- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

---

<sup>23</sup> How to Protect Your Networks from RANSOMWARE, at 3–4, *available at* <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Feb. 22, 2023).

- Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . . .<sup>24</sup>

113. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- Secure internet-facing assets
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- Thoroughly investigate and remediate alerts
  - Prioritize and treat commodity malware infections as potential full compromise;
- Include IT Pros in security discussions
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely
- Build credential hygiene

---

<sup>24</sup> See *Security Tip* (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Feb. 22, 2023).



- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege
- Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- Harden infrastructure
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].<sup>25</sup>

114. Moreover, given that Defendant was storing PII of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

115. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

116. As a result of computer systems in need of security upgrades, as well as inadequate procedures for handling email phishing attacks, viruses, malignant computer code, and hacking

---

<sup>25</sup> See *Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last accessed Feb. 22, 2023).

1 attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members'  
2 PII.

3 117. Because Defendant failed to properly protect and safeguard Plaintiffs' and Class  
4 Members' PII, an unauthorized third party was able to access Defendant's network and access  
5 Defendant's database and system configuration files and exfiltrate that data.

6 ***ii. Defendant Failed to Comply with FTC Guidelines***

7 118. The Federal Trade Commission ("FTC") has promulgated numerous guides for  
8 businesses that highlight the importance of implementing reasonable data security practices.  
9 According to the FTC, the need for data security should be factored into all business decision  
10 making.

11 119. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide*  
12 *for Business*, which established cyber-security guidelines for businesses. The guidelines note that  
13 businesses should protect the personal information that they keep; properly dispose of personal  
14 information that is no longer needed; encrypt information stored on computer networks;  
15 understand their network's vulnerabilities; and implement policies to correct any security  
16 problems.<sup>26</sup>

17 120. The guidelines also recommend that businesses use an intrusion detection system  
18 to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone  
19 is attempting to hack the system; watch for large amounts of data being transmitted from the  
20 system; and have a response plan ready in the event of a breach.

21 121. The FTC further recommends that companies not maintain PII longer than is  
22 needed for authorization of a transaction; limit access to sensitive data; require complex passwords  
23 to be used on networks; use industry-tested methods for security; monitor for suspicious activity

24  
25 <sup>26</sup> *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (2016),  
26 available at <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>.

1 on the network; and verify that third-party service providers have implemented reasonable security  
2 measures.

3 122. The FTC has brought enforcement actions against businesses for failing to  
4 adequately and reasonably protect consumers' data, treating the failure to employ reasonable and  
5 appropriate measures to protect against unauthorized access to confidential consumer data as an  
6 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15  
7 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their  
8 data security obligations.

9 123. Defendant failed to properly implement basic data security practices.

10 124. Defendant's failure to employ reasonable and appropriate measures to protect  
11 against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or  
12 practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

13 125. Defendant was always fully aware of its obligation to protect the PII of Plaintiff  
14 and Class Members. Defendant was also aware of the significant repercussions that would result  
15 from its failure to do so.

16 ***iii. Defendant Failed to Comply with Industry Standards***

17 126. As shown above, experts studying cyber security routinely identify entities like  
18 RPM as being particularly vulnerable to cyberattacks because of the value of the PII that they  
19 collect and maintain.

20 127. Several best practices have been identified that at a minimum should be  
21 implemented by businesses like Defendant, including, but not limited to: educating all employees;  
22 requiring strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware  
23 software; encryption, making data unreadable without a key; multi-factor authentication; backup  
24 data; and limiting which employees can access sensitive data.

25 128. Other best cybersecurity practices include installing appropriate malware detection  
26 software; monitoring and limiting the network ports; protecting web browsers and email

1 management systems; setting up network systems such as firewalls, switches and routers;  
 2 monitoring and protection of physical security systems; protection against any possible  
 3 communication system; and training staff regarding critical points.

4 129. Defendant failed to meet the minimum standards of any of the following  
 5 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation  
 6 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,  
 7 PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for  
 8 Internet Security's Critical Security Controls (CIS CSC), which are all established standards in  
 9 reasonable cybersecurity readiness.

10 130. The foregoing frameworks are existing and applicable industry standards, and  
 11 Defendant failed to comply with these accepted standards, thereby opening the door to and causing  
 12 the Data Breach.

13 131. Upon information and belief, Defendant failed to comply with one or more of the  
 14 foregoing industry standards.

### 15 **COMMON INJURIES & DAMAGES**

16 132. As result of Defendant's ineffective and inadequate data security practices,  
 17 Plaintiffs and Class Members now face a present and ongoing imminent risk of fraud and identity  
 18 theft.

19 133. Due to the Data Breach, and the foreseeable consequences of PII ending up in the  
 20 possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized  
 21 and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages,  
 22 including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized  
 23 risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred  
 24 mitigating the materialized risk and imminent threat of identity theft; (d) "out of pocket" costs  
 25 incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss  
 26 of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain

(price premium damages); (h) diminution of value of their PII; and (i) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

**A. The Risk of Identity Theft and Fraud to Plaintiffs and Class Members Is Present and Ongoing**

134. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

135. Because a person's identity is akin to a puzzle with multiple data points, the greater the number of accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity directly, or to track the victim to attempt other hacking crimes that will allow them to obtain more data to perfect a crime.

136. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously-acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

137. The dark web is an unindexed layer of the internet that requires special software or authentication to access.<sup>27</sup> Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web

---

<sup>27</sup> *What Is the Dark Web?*, EXPERIAN (May 12, 2021), available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

1 users need to know the web address of the website they wish to visit in advance. For example, on  
 2 the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is  
 3 ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.<sup>28</sup> This prevents dark web  
 4 marketplaces from being easily monitored by authorities or accessed by those not in the know.

5 138. A sophisticated black market exists on the dark web where criminals can buy or  
 6 sell malware, firearms, drugs, and frequently, personal and medical information like the PII at  
 7 issue here.<sup>29</sup> The digital character of PII stolen in data breaches, specifically this Data Breach,  
 8 lends itself to dark web transactions because it is immediately transmissible over the internet and  
 9 the buyer and seller can retain their anonymity. The sale of a firearm or drugs, on the other hand,  
 10 requires a physical delivery address. Nefarious actors can readily purchase usernames and  
 11 passwords for online streaming services, stolen financial information and account login  
 12 credentials, and Social Security numbers, dates of birth, and medical information.<sup>30</sup> As Microsoft  
 13 warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial  
 14 harm to others."<sup>31</sup>

15 139. Identity thieves can also use Social Security numbers to obtain a driver's license or  
 16 official identification card in the victim's name but with the thief's picture; use the victim's name  
 17 and Social Security number to obtain government benefits; or file a fraudulent tax return using the  
 18 victim's information. In addition, identity thieves may obtain a job using the victim's Social  
 19 Security number, rent a house, or receive medical services in the victim's name, and may even  
 20 give the victim's personal information to police during an arrest resulting in an arrest warrant being

---

21 <sup>28</sup> *Id.*

22 <sup>29</sup> *What is the Dark Web?*, MICROSOFT 365 (July 15, 2022), *available at*  
 23 <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

24 <sup>30</sup> *Id.*; *What Is the Dark Web?*, EXPERIAN (May 12, 2021), *available at*  
 25 <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

26 <sup>31</sup> *What is the Dark Web?*, MICROSOFT 365 (July 15, 2022), *available at*  
<https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

1 issued in the victim's name. The Social Security Administration has warned that identity thieves  
2 can also use an individual's Social Security number to apply for additional credit lines.<sup>32</sup>

3 140. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime  
4 Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that  
5 year, resulting in more than \$3.5 billion in losses to individuals and business victims.<sup>33</sup>

6 141. Further, according to the same report, "rapid reporting can help law enforcement  
7 stop fraudulent transactions before a victim loses the money for good."<sup>34</sup> Defendant did not rapidly  
8 report to Plaintiffs and the Class that their PII had been stolen.

9 142. Victims of identity theft also often suffer embarrassment, blackmail, or harassment  
10 in person or online, and/or experience financial losses resulting from fraudulently opened accounts  
11 or misuse of existing accounts.

12 143. In addition to out-of-pocket expenses that can exceed thousands of dollars and the  
13 emotional toll identity theft can take, some victims have to spend a considerable time repairing the  
14 damage caused by the theft of their PII. Victims of new account identity theft will likely have to  
15 spend time correcting fraudulent information in their credit reports and continuously monitor their  
16 reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute  
17 charges with creditors.

18 144. Further complicating the issues faced by victims of identity theft, data thieves may  
19 wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class  
20 Members will need to be remain vigilant against unauthorized data use for years or even decades  
21 to come.

22  
23  
24 <sup>32</sup> *Identity Theft and Your Social Security Number*, SOC. SEC. ADMIN. (2018) at 1,  
available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Feb. 22, 2023).

25 <sup>33</sup> See *2019 Internet Crime Report Released* (Feb. 11, 2020), [https://www.fbi.gov/news/](https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120)  
26 stories/2019-internet-crime-report-released-021120 (last accessed Feb. 22, 2023).

<sup>34</sup> *Id.*

1           145. The FTC has also recognized that consumer data is a new and valuable form of  
 2 currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated  
 3 that “most consumers cannot begin to comprehend the types and amount of information collected  
 4 by businesses, or why their information may be commercially valuable. Data is currency. The  
 5 larger the data set, the greater potential for analysis and profit.”<sup>35</sup>

6           146. The FTC has also issued numerous guidelines for businesses that highlight the  
 7 importance of reasonable data security practices. The FTC has noted the need to factor data  
 8 security into all business decision-making. According to the FTC, data security requires: (1)  
 9 encrypting information stored on computer networks; (2) retaining payment card information only  
 10 as long as necessary; (3) properly disposing of personal information that is no longer needed; (4)  
 11 limiting administrative access to business systems; (5) using industry-tested and accepted methods  
 12 for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7)  
 13 verifying that privacy and security features function properly; (8) testing for common  
 14 vulnerabilities; and (9) updating and patching third-party software.<sup>36</sup>

15           147. Defendant’s failure to properly notify Plaintiffs and Class Members of the Data  
 16 Breach exacerbated Plaintiffs’ and Class Members’ injury by depriving them of the earliest ability  
 17 to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm  
 18 caused by the Data Breach.

#### 19           **B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud**

20           148. As a result of the recognized risk of identity theft, when a Data Breach occurs and  
 21 an individual is notified by a company that their PII was compromised, as in this Data Breach, the  
 22 reasonable person is expected to take steps and spend time to address the dangerous situation, learn  
 23

---

24           <sup>35</sup> Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy*  
 25 *Roundtable* (Dec. 7, 2009), [https://www.ftc.gov/sites/default/files/documents/public\\_statements/](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf)  
 26 [remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf) (last visited Feb. 22,  
 2023).

<sup>36</sup> See generally *Protecting Personal Information*, *supra* note 26.



1 about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud.  
 2 Failure to spend time taking steps to review accounts or credit reports could expose the individual  
 3 to greater financial harm—yet the resource and asset of time has been lost.

4 149. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class  
 5 Members must, as Defendant’s Data Breach Notice instructs them to do, “closely monitor all mail,  
 6 email, and other contact from individuals not known to you personally” and to “remain vigilant  
 7 for fraud or identity theft by reviewing account statements, explanation of benefits statements, and  
 8 credit reports for unauthorized activity . . . .”

9 150. Plaintiffs and Class Members have spent time, and will spend additional time in the  
 10 future, on a variety of prudent actions, such as placing “freezes” and “alerts” with credit reporting  
 11 agencies, contacting financial institutions, closing, or modifying financial accounts, changing  
 12 passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and  
 13 filing police reports.

14 151. Plaintiffs’ mitigation efforts are consistent with guidance from the U.S.  
 15 Government Accountability Office, which released a report in 2007 regarding data breaches  
 16 (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and  
 17 time to repair the damage to their good name and credit record.”<sup>37</sup>

18 152. Plaintiffs’ mitigation efforts are also consistent with the steps that FTC  
 19 recommends that data breach victims take to protect their personal and financial information after  
 20 a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider  
 21 an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their  
 22 credit reports, contacting companies to remove fraudulent charges from their accounts, placing a  
 23  
 24

---

25 <sup>37</sup> See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting*  
 26 *Identity Theft Is Limited; However, the Full Extent Is Unknown* GAO-07-737, U.S. GOV’T  
 ACCOUNTABILITY OFFICE, (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

1 credit freeze on their credit, and correcting their credit reports.<sup>38</sup>

### 2 **C. Diminution of Value of the PII**

3 153. PII is a valuable property right.<sup>39</sup> Considering the value of Big Data in corporate  
4 America, and the potential consequences to cyber thieves (including heavy prison sentences), its  
5 value is axiomatic. Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has  
6 considerable market value.

7 154. Sensitive PII can sell for as much as \$363 per record according to the Infosec  
8 Institute.<sup>40</sup>

9 155. An active and robust legitimate marketplace for PII also exists. In 2019, the data  
10 brokering industry was worth roughly \$200 billion.<sup>41</sup> In fact, the data marketplace is so  
11 sophisticated that consumers can actually sell their non-public information directly to a data  
12 broker, who in turn aggregates the information and provides it to marketers or app developers.<sup>42</sup>  
13 Consumers who agree to provide their web browsing history to the Nielsen Corporation can  
14 receive up to \$50.00 a year.<sup>43</sup>

15 156. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an  
16 inherent market value in both legitimate and black markets, has been damaged and diminished by  
17

---

18 <sup>38</sup> See FED. TRADE COMM'N, IDENTITY THEFT.GOV, <https://www.identitytheft.gov/Steps>  
19 (last visited Feb. 22, 2023).

20 <sup>39</sup> See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally*  
21 *Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH.  
22 11, at \*3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is  
23 rapidly reaching a level comparable to the value of traditional financial assets." (citations  
24 omitted)).

25 <sup>40</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27,  
26 2015), [https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-](https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/)  
market/ (last visited Feb. 22, 2023).

<sup>41</sup> David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak* (Nov.  
5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

<sup>42</sup> See, e.g., <https://datacoup.com/>; <https://worlddataexchange.com/about>.

<sup>43</sup> Computer & Mobile Panel, NIELSEN, available at <https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing> (last visited Feb. 22, 2023).

1 its unauthorized release onto the Dark Web, where it is now available and holds significant value  
2 for the threat actors. However, this transfer of value occurred without any consideration paid to  
3 Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is  
4 now readily available, and the rarity of Plaintiffs' and Class Members' PII has been lost, thereby  
5 causing additional loss of value.

6 **D. Future Cost of Credit and Identify Theft Monitoring Is Reasonable and**  
7 **Necessary**

8 157. To date, Defendant has done little to provide Plaintiffs and Class Members with  
9 relief for the damages they have suffered as a result of the Data Breach—Defendant has offered  
10 only 12 months of inadequate identity monitoring services, despite Plaintiffs and Class Members  
11 being at risk of identity theft and fraud for the foreseeable future. Defendant has not offered any  
12 other relief or protection.

13 158. The 12 months of credit monitoring offered to persons whose PII was compromised  
14 is wholly inadequate as it fails to provide for the fact that victims of data breaches and other  
15 unauthorized disclosures commonly face multiple years of ongoing identity theft and financial  
16 fraud. Defendant also places the burden squarely on Plaintiffs and Class Members by requiring  
17 them to expend time signing up for that service, as opposed to automatically enrolling all victims  
18 of this Data Breach.

19 159. Given the type of targeted attack in this case and sophisticated criminal activity,  
20 the type of PII, reports of misuse of Plaintiffs' PII discussed above, and reports of dissemination  
21 on the Dark Web also discussed above, there is a strong probability that entire batches of stolen  
22 information have been placed, or will be placed, on the black market/dark web for sale and  
23 purchase by criminals intending to utilize the PII for identity theft crimes, including opening bank  
24 accounts in the victims' names to make purchases or to launder money; file false tax returns; take  
25 out loans or lines of credit; or file false unemployment claims.

1           160. Such fraud may go undetected until debt collection calls commence months, or even  
 2 years, later. An individual may not know that his or her Social Security Number was used to file  
 3 for unemployment benefits until law enforcement notifies the individual's employer of the  
 4 suspected fraud. Fraudulent tax returns are typically discovered only when an individual's  
 5 authentic tax return is rejected.

6           161. Furthermore, the information accessed and disseminated in the Data Breach is  
 7 significantly more valuable than the loss of, for example, credit card information in a retailer data  
 8 breach, where victims can easily cancel or close credit and debit card accounts.<sup>44</sup> The information  
 9 disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change  
 10 (such as Social Security numbers).

11           162. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of  
 12 fraud and identity theft for many years into the future.

13           163. The retail cost of credit monitoring and identity theft monitoring can cost around  
 14 \$200 a year per Class Member. This is a reasonable and necessary cost towards protecting Class  
 15 Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future  
 16 cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for  
 17 Defendant's failure to safeguard their PII.

#### 18           **E. Injunctive Relief Is Necessary to Protect Against Future Data Breaches**

19           164. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII,  
 20 which is believed to remain in the possession of Defendant, is protected from further breaches by  
 21 the implementation of security measures and safeguards, including but not limited to, making sure  
 22 that the storage of data or documents containing PII is not accessible online and that access to such  
 23 data is password protected.

---

25           <sup>44</sup> See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New*  
 26 *Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

**CLASS ACTION ALLEGATIONS**

165. Plaintiffs bring this action under Federal Rule of Civil Procedure 23 against Defendant individually and on behalf of all others similarly situated. Plaintiffs assert all claims on behalf of the Class, defined as follows:

**Nationwide Class**

All persons residing in the United States whose personally identifiable information was accessed or acquired as a result of the Data Breach that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and other Class Members on or around November 21, 2022 (the “Nationwide Class”).

166. Plaintiffs also seek to represent the following state subclass defined as:

**Georgia Subclass**

All Georgia residents whose personally identifiable information was accessed or acquired as a result of the Data Breach that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and other Class Members on or around November 21, 2022 (the “Georgia Subclass”).

167. The Nationwide Class and the state Subclass are referred to collectively as the Class. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant’s officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

168. Plaintiffs reserve the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

169. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

170. Numerosity: The proposed Class is believed to be so numerous that joinder of all members is impracticable. Indeed, Defendant has disclosed that in total, the Data Breach

1 compromised the PII of approximately 3,766,573 people, including Plaintiffs and Class  
2 Members.<sup>45</sup>

3 171. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all  
4 members of the Class were injured through Defendant's uniform misconduct. The same event and  
5 conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every  
6 other Class Member because Plaintiffs and each member of the Class had their sensitive PII  
7 compromised in the same way by the same conduct of Defendant.

8 172. Adequacy: Plaintiffs are adequate representatives of the Class because Plaintiffs'  
9 interests do not conflict with the interests of the Class they seek to represent; Plaintiffs have  
10 retained counsel competent and highly experienced in data breach class action litigation; and  
11 Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the  
12 Class will be fairly and adequately protected by Plaintiffs and Plaintiffs' counsel.

13 173. Superiority: A class action is superior to other available means of fair and efficient  
14 adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class  
15 Member is relatively small in comparison to the burden and expense of individual prosecution of  
16 complex and expensive litigation. It would be very difficult, if not impossible, for members of the  
17 Class to individually and effectively redress Defendant's wrongdoing. Even if Class Members  
18 could afford such individual litigation, the court system could not. Individualized litigation  
19 presents a potential for inconsistent or contradictory judgments. Individualized litigation increases  
20 the delay and expense to all parties, and to the court system, presented by the complex legal and  
21 factual issues of the case. By contrast, the class action device presents far fewer management  
22 difficulties and provides benefits of single adjudication, economy of scale, and comprehensive  
23 supervision by a single court.

24  
25  
26 <sup>45</sup>See Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aewviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml> (last visited Feb. 16, 2023).

1           174. Commonality and Predominance: There are many questions of law and fact  
 2 common to the claims of Plaintiffs and the other members of the Class, and those questions  
 3 predominate over any questions that may affect individual members of the Class. Common  
 4 questions for the Class include:

- 5           a. Whether Defendant engaged in the wrongful conduct alleged herein;
- 6           b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class  
 7           Members' PII;
- 8           c. Whether Defendant's computer systems and data security practices used to  
 9           protect Plaintiffs' and Class Members' PII violated the FTC Act, and/or  
 10           state laws and/or Defendant' other duties discussed herein;
- 11           d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately  
 12           protect their PII, and whether it breached this duty;
- 13           e. Whether Defendant knew or should have known that its computer and  
 14           network security systems were vulnerable to a data breach or disclosure;
- 15           f. Whether Defendant's conduct, including its failure to act, resulted in or was  
 16           the proximate cause of the Data Breach;
- 17           g. Whether Defendant breached contractual duties to Plaintiffs and the Class  
 18           to use reasonable care in protecting their PII;
- 19           h. Whether Defendant failed to adequately respond to the Data Breach,  
 20           including failing to investigate it diligently and notify affected individuals  
 21           in the most expedient time possible and without unreasonable delay, and  
 22           whether this caused damages to Plaintiffs and the Class;
- 23           i. Whether Plaintiffs and the Class suffered injury as a proximate result of  
 24           Defendant's negligent actions or failures to act;
- 25           j. Whether Plaintiffs and the Class are entitled to recover damages, equitable  
 26           relief, and other relief;

- 1 k. Whether injunctive relief is appropriate and, if so, what injunctive relief is  
2 necessary to redress the imminent and currently ongoing harm faced by  
3 Plaintiffs and members of the Class; and  
4 l. Whether Plaintiffs and Class Members are entitled to treble damages.

5 **CAUSES OF ACTION**

6 **FIRST CAUSE OF ACTION**

7 **NEGLIGENCE**

8 **(On Behalf of Plaintiffs and the Nationwide Class)**

9 175. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth  
10 herein.

11 176. Defendant gathered and stored the PII of Plaintiffs and the Class as part of the  
12 operation of its business and benefited from holding and using the PII in its business operations.

13 177. Upon accepting, storing, and utilizing the PII of Plaintiffs and Class Members for  
14 its benefit, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise  
15 reasonable care to secure and safeguard that information and to use secure methods and to  
16 implement necessary data security protocols and employee training to do so.

17 178. Defendant had full knowledge of the sensitivity of the PII, the types of harm that  
18 Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed, the  
19 importance of adequate data security, and of prior data breaches.

20 179. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety  
21 and security practices. Plaintiffs and the Class Members had no ability to protect their PII that was  
22 in Defendant's possession. As such, a special relationship existed between Defendant and  
23 Plaintiffs and the Class.

24 180. Defendant owed Plaintiffs and Class Members a common law duty to use  
25 reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when  
26 obtaining, storing, using, and managing their PII, including taking action to reasonably safeguard



1 such data and providing notification to Plaintiffs and the Class Members of any breach in a timely  
2 manner so that appropriate action could be taken to minimize losses.

3 181. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of  
4 foreseeable criminal conduct of third parties, which has been recognized in situations where the  
5 actor's own conduct or misconduct exposes another to the risk or defeats protections put in place  
6 to guard against the risk, or where the parties are in a special relationship. *See* Restatement  
7 (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of  
8 a specific duty to reasonably safeguard personal information.

9 182. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class  
10 from being vulnerable to compromise by taking common-sense precautions when dealing with  
11 sensitive PII. Additional duties that Defendant owed Plaintiffs and the Class include:

- 12 a. To exercise reasonable care in designing, implementing, maintaining,  
13 monitoring, and testing Defendant's networks, systems, protocols, policies,  
14 procedures and practices to ensure that Plaintiffs' and Class Members' PII was  
15 adequately secured from impermissible release, disclosure, and publication;  
16 b. To protect Plaintiffs' and Class Members' PII in its possession by using  
17 reasonable and adequate security procedures and systems; and  
18 c. To promptly notify Plaintiffs and Class Members of any breach, security  
19 incident, unauthorized disclosure, or intrusion that affected or may have  
20 affected their PII.

21 183. Defendant also had a duty to protect Plaintiffs' and the Class's PII because  
22 Defendant engaged in an affirmative act or misfeasance such that it increased the risk of financial  
23 harm to the Plaintiffs and otherwise created a situation of peril for Plaintiffs and the Class.  
24 Defendant knowingly and deliberately chose not to employ adequate data security to save on costs,  
25 despite being on notice of rampant data breaches across the country. These negligent acts placed  
26 Plaintiffs and Class Members at an imminent risk of identity theft and fraud and created a situation

1 of peril for Plaintiffs and the Class by leaving their PII vulnerable to exposure and theft by criminal  
2 actors.

3 184. Only Defendant was in a position to ensure that its data systems and protocols were  
4 sufficient to protect the PII that had been entrusted to it.

5 185. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and  
6 Class Members' PII. Defendant breached its duties by, among other things:

- 7 a. Failing to exercise reasonable care in obtaining, retaining, securing,  
8 safeguarding, protecting, and deleting the PII in its possession;
- 9 b. Failing to protect the PII in its possession using reasonable and adequate  
10 security procedures and systems;
- 11 c. Failing to adequately and properly audit, test, and train its employees regarding  
12 how to properly and securely transmit and store PII;
- 13 d. Failing to adequately train its employees to not store unencrypted PII in their  
14 personal files longer than absolutely necessary for the specific purpose that it  
15 was sent or received;
- 16 e. Failing to consistently enforce security policies aimed at protecting Plaintiffs'  
17 and the Class's PII;
- 18 f. Failing to mitigate the harm caused to Plaintiffs and the Class Members;
- 19 g. Failing to implement processes to quickly detect data breaches, security  
20 incidents, or intrusions; and
- 21 h. Failing to promptly notify Plaintiffs and Class Members of the Data Breach  
22 that affected their PII.

23 186. Defendant's willful failure to abide by these duties was wrongful, reckless, and  
24 grossly negligent in light of the foreseeable risks and known threats.

1           187. As a proximate and foreseeable result of Defendant's negligent conduct, Plaintiffs  
2 and the Class have suffered damages and are at imminent risk of identity theft, fraud, and additional  
3 harms and damages (as alleged above).

4           188. Through Defendant's acts and omissions described herein, including but not limited  
5 to Defendant's failure to protect the PII of Plaintiffs and Class Members from being stolen and  
6 misused and published on the dark web, Defendant unlawfully breached its duty to use reasonable  
7 care to adequately protect and secure the PII of Plaintiffs and Class Members while it was within  
8 Defendant's possession and control.

9           189. Further, through its failure to provide timely and clear notification of the Data  
10 Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from  
11 taking meaningful, proactive steps to secure their PII and mitigate damages.

12           190. As a result of the Data Breach and subsequent notification letters, Plaintiffs and  
13 Class Members have spent time, effort, and money to mitigate the actual and potential impact of  
14 the Data Breach on their lives, including but not limited to, responding to the fraudulent use of  
15 their PII and closely reviewing and monitoring bank accounts, credit reports, and financial  
16 statements.

17           191. Defendant's wrongful actions, inaction, and omissions constituted (and continue to  
18 constitute) common law negligence and recklessness.

19           192. The damages Plaintiffs and the Class have suffered (as alleged above) and will  
20 suffer were and are the direct and proximate result of Defendant's negligent and reckless conduct.

21           193. Plaintiffs and the Class have suffered actual injury and are entitled to compensatory  
22 damages in amounts to be proven at trial.

**SECOND CAUSE OF ACTION  
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT  
(On Behalf of Plaintiffs and the Nationwide Class)**

194. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

195. Defendant entered into various written contracts with its clients to perform services that include, but are not limited to, debt recovery services.

196. These contracts were made in part for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. The contracts were made with the intent and expectation that Plaintiffs' and Class Members' PII would remain private and would be adequately protected from unauthorized disclosure. Indeed, Defendant knew that if it were to breach these contracts with its clients, the clients' customers—Plaintiffs and Class Members—would be harmed.

197. It was intended by Defendant and its clients at the time the contracts were made that Defendant would assume a direct obligation to protect Plaintiffs' and the Class's PII.

198. It was also intended by Defendant and its clients that the performance under the contract would necessarily and directly benefit Plaintiffs and the Class. Defendant would collect payment from Plaintiffs and the Class and Defendant would expunge their debt in return.

199. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures and (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' PII from unauthorized disclosure to third parties.

200. As foreseen, Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to compensatory damages they have sustained as a direct and proximate result thereof.

**THIRD CAUSE OF ACTION**  
**VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT (RCW 19.86.010 ET SEQ.)**  
**(On Behalf of the Nationwide Class)**

201. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

202. The Washington State Consumer Protection Act, RCW 19.86.020 (the “CPA”) prohibits any “unfair or deceptive acts or practices” in the conduct of any trade or commerce. The CPA does not define “unfair” or “deceptive.”

203. Either an unfair or a deceptive act or practice may serve as the basis of a CPA claim. *See Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1161 (W.D. Wash. 2017) (citation omitted).

204. Defendant is a “person” as described in RCW 19.86.010(1).

205. Defendant engages in “trade” and “commerce” as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

206. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people of the State of Washington.

207. In the course of conducting its business, Defendant committed “unfair acts or practices” by, among other things, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs’ and Class Members’ PII. Plaintiffs and the Class reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant’s unfair acts and practices are ongoing and continue to this date.

208. These unfair acts have caused substantial injury to Plaintiffs and the Class because

1 their PII has been exposed to cyber criminals who will commit identity theft and fraud. Plaintiffs  
2 and the Class were unable to avoid Defendant servicing their accounts because Defendant was  
3 selected by its clients. Further, Defendant's unfair acts have no countervailing benefits; Plaintiffs  
4 and the Class will not benefit from the exposure of their PII.

5 209. Defendant's conduct was also deceptive. Defendant concealed from Plaintiffs and  
6 Class Members the unauthorized release and disclosure of their PII, and it failed to timely notify  
7 them of that unauthorized release and disclosure. If Plaintiffs and Class Members had been notified  
8 in an appropriate fashion, and had the information not been hidden from them, they could have  
9 taken precautions to safeguard and protect their PII.

10 210. Defendant's above-described "unfair or deceptive acts or practices" affects the  
11 public interest because it is substantially injurious to persons and has the capacity to injure other  
12 persons.

13 211. The gravity of Defendant's wrongful conduct outweighs any alleged benefits  
14 attributable to such conduct. There were reasonably available alternatives to further Defendant's  
15 legitimate business interests other than engaging in the above-described wrongful conduct.

16 212. Defendant's above-described unfair and deceptive acts and practices directly and  
17 proximately caused injury to Plaintiffs' and Class Members' business and property. Plaintiffs and  
18 Class Members have suffered, and will continue to suffer, actual damages and injury in the form  
19 of, among other things, (1) an imminent, immediate, and continuing increased risk of identity theft  
20 and identity fraud—risks justifying expenditures for protective and remedial services for which  
21 Plaintiffs and Class Members are entitled to compensation; (2) invasion of privacy; (3) breach of  
22 the confidentiality of Plaintiffs' and Class Members' PII; (5) deprivation of the value of Plaintiffs'  
23 and Class Members' PII, for which there is a well-established national and international market;  
24 (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and  
25 mitigating damages; and/or (7) investment of substantial time and money to monitoring and  
26 remediating the harm inflicted upon them.

1           213. Unless restrained and enjoined, Defendant will continue to engage in the above-  
 2 described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of  
 3 themselves, Class Members, and the general public, also seek restitution and an injunction  
 4 prohibiting Defendant from continuing such wrongful conduct and requiring Defendant to modify  
 5 its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor, and  
 6 audit appropriate data security processes, controls, policies, procedures, protocols, and software  
 7 and hardware systems to safeguard and protect the PII entrusted to it.

8           214. Plaintiffs and Class Members also seek to recover actual damages sustained by each  
 9 Class Member together with the costs of the suit, including reasonable attorneys' fees.

10           215. In addition, Plaintiffs, on behalf of themselves and the Class Members, request that  
 11 this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each  
 12 Class Member by three times the actual damages sustained, not to exceed \$25,000.00 per Class  
 13 Member.

14                                   **FOURTH CAUSE OF ACTION**  
 15                   **VIOLATIONS OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT,**  
 16                                   **O.C.G.A. § 10-1-912, ET SEQ.**  
                                   **(On behalf of Plaintiff Dean and the Georgia Subclass)**

17           216. Plaintiff Dean ("Plaintiff," for purposes of this Count) incorporates by reference  
 18 the foregoing paragraphs as if fully set forth herein.

19           217. Plaintiff brings this count on behalf of the Georgia Subclass.

20           218. Defendant is a business that owns or licenses computerized data that includes PII  
 21 as defined by O.C.G.A. § 10-1-912(a).

22           219. Plaintiff and Georgia Subclass Members' PII that was compromised in the Data  
 23 Breach includes PII covered under O.C.G.A. § 10-1-912(a).

24           220. Defendant is required to accurately notify Plaintiff and Georgia Subclass Members  
 25 if it becomes aware of a breach of its data security systems that was reasonably likely to have  
 26

1 caused unauthorized persons to acquire Plaintiff's and Georgia Subclass Members' PII in the most  
2 expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

3 221. By failing to disclose the Data Breach in a timely and accurate manner, Defendant  
4 violated O.C.G.A. § 10-1-912(a).

5 222. As a direct and proximate result of Defendants' violations of O.C.G.A. § 10-1-  
6 912(a), Plaintiff and Georgia Subclass members suffered damages, as described above.

7 223. Plaintiff and Georgia Subclass members seek relief under O.C.G.A. § 10-1-912,  
8 including actual damages and injunctive relief.

9  
10 **FIFTH CAUSE OF ACTION**  
11 **VIOLATIONS OF THE GEORGIA DECEPTIVE PRACTICES ACT,**  
12 **GA. CODE ANN. §§ 10-1-370, *ET SEQ.***  
13 **(On behalf of Plaintiff Dean and the Georgia Subclass)**

14 224. Plaintiff Dean ("Plaintiff," for purposes of this Count) and the Georgia Subclass  
15 incorporate by reference the foregoing paragraphs as if fully set forth herein.

16 225. RPM, Plaintiff, and the Georgia Subclass members are "persons" within the  
17 meaning of the Georgia Deceptive Trade Practices Act ("Georgia DTPA"), Ga. Code Ann. § 10-  
18 1-370(5).

19 226. The Georgia DTPA states the following at Ga. Code Ann. § 10-1-372:

20 (a) A person engages in a deceptive trade practice when, in the course of his  
21 business, vocation, or occupation, he: . . . (5) Represents that goods or services have  
22 . . . characteristics, . . . uses, [or] benefits . . . that they do not have; . . . (7) Represents  
23 that goods or services are of a particular standard, quality, or grade . . . if they are  
24 of another; . . . [or] (12) Engages in any other conduct which similarly creates a  
25 likelihood of confusion or of misunderstanding.

26 227. RPM engaged in deceptive trade practices in violation of Ga. Code Ann. § 10-1-  
372(a)(5), (7), and (12) by, among other things:

(a) Omitting and concealing the material fact that it did not employ reasonable  
measures to secure consumers' PII. RPM could and should have made a proper disclosure  
to consumers (including its clients and Georgia Subclass Members), during its engagement



1 process or debt collection process, or by any other means reasonably calculated to inform  
2 consumers of the inadequate data security; and

3 (b) Making implied or implicit representations that its data security practices were  
4 sufficient to protect consumers' PII. RPM acquired consumers' PII during the debt  
5 collection process. In doing so, RPM made implied or implicit representations that its data  
6 security practices were sufficient to protect consumers' PII. By virtue of accepting  
7 Plaintiffs' PII during the collection process, RPM implicitly represented (including to  
8 RPM's clients who may not have elected to use RPM for their collections had they known  
9 the true state of affairs) that its data security processes were sufficient to safeguard the PII.

10 228. The Georgia DTPA states that "[i]n order to prevail in an action under this part, a  
11 complainant need not prove . . . actual confusion or misunderstanding." Ga. Code Ann. § 10-1-  
12 372(b).

13 229. The Georgia DTPA further states: "A person likely to be damaged by a deceptive  
14 trade practice of another may be granted an injunction against it under the principles of equity and  
15 on terms that the court considers reasonable. Proof of monetary damage, loss of profits, or intent  
16 to deceive is not required." Ga. Code Ann. § 10-1-373(a).

17 230. While Defendant provided notice of the Data Breach, Defendant has not provided  
18 sufficient details regarding the full scope of the Data Breach or any details related to the remedial  
19 measures that it has taken to improve and more fully safeguard Plaintiffs' and Georgia Subclass  
20 Members' data from future compromise. As a result, Plaintiffs, Georgia Subclass Members, and  
21 RPM's clients remain uninformed and confused as to the adequacy of RPM's data security and  
22 RPM's ability to protect the PII entrusted to it. Without adequate improvements, Plaintiffs' and  
23 Georgia Subclass' Members data remains at an unreasonable risk for future compromise.

24 231. Moreover, Defendant, through its omissions and Notice Letter, continues to  
25 represent and imply that its data security measures are adequate to protect the PII of Plaintiff and  
26 the Georgia Subclass. Such continued representations and implications, without disclosure of the

1 full scope of the Data Breach or remedial enhancements, place Plaintiffs and Georgia Subclass  
2 Members at a future risk of harm, as Plaintiffs, Georgia Subclass Members, and RPM's clients are  
3 not fully informed as to whether RPM's data security measures have been improved since the Data  
4 Breach. By all available measures, RPM's data systems have not been adequately improved, and  
5 Plaintiffs and Georgia Subclass Members remain at an unreasonable risk from future cyberattacks.

6 232. Plaintiffs and the Georgia Subclass, therefore, are entitled to the injunctive relief  
7 sought herein because, among other things, RPM continues to retain their PII, future cyber-attacks  
8 targeting the same data are foreseeable, and Defendants have not provided sufficient notice  
9 identifying any remedial measures that will protect the data from future attack. Moreover, absent  
10 injunctive relief, Defendant will continue to misrepresent and imply that its data systems are  
11 adequate to protect the PII of Plaintiffs and the Georgia Subclass from future cyberattacks without  
12 providing any firm details or basis to support these representations.

13 233. The Georgia DTPA states that the "court, in its discretion, may award attorney's  
14 fees to the prevailing party if . . . [t]he party charged with a deceptive trade practice has willfully  
15 engaged in the trade practice knowing it to be deceptive." Ga. Code Ann. § 10-1-373(b)(2). RPM  
16 willfully engaged in deceptive trade practices knowing them to be deceptive. RPM knew or should  
17 have known that its data security practices were deficient. This is true because, among other things,  
18 RPM was aware that entities responsible for collecting and maintaining large amounts of PII,  
19 including Social Security numbers and financial information, are frequent targets of sophisticated  
20 cyberattacks. RPM knew or should have known that its data security practices were insufficient to  
21 guard against those attacks.

22 234. The Georgia DTPA states that "[c]osts shall be allowed to the prevailing party  
23 unless the court otherwise directs." Ga. Code Ann. § 10-1-373(b). Plaintiff and the Georgia  
24 Subclass are entitled to recover their costs of pursuing this litigation.



1           244. Actual harm has arisen in the wake of the Data Breach regarding Defendant's  
 2 contractual obligations and duties of care to provide security measures to Plaintiffs and the  
 3 members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or  
 4 further harm due to the exposure of their PII and Defendant's failure to address the security failings  
 5 that led to such exposure.

6           245. There is no reason to believe that Defendant's employee training and security  
 7 measures are any more adequate now than they were before the Data Breach to meet Defendant's  
 8 contractual obligations and legal duties.

9           246. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendant's existing  
 10 data security measures do not comply with its contractual obligations and duties of care to provide  
 11 adequate data security, and (2) that to comply with its contractual obligations and duties of care,  
 12 Defendant must implement and maintain reasonable security measures, including, but not limited  
 13 to, the following:

- 14           a. Ordering that Defendant engage internal security personnel to conduct testing,  
 15           including audits on Defendant's systems, on a periodic basis, and ordering  
 16           Defendant to promptly correct any problems or issues detected by such third-party  
 17           security auditors;
- 18           b. Ordering that Defendant engage third-party security auditors and internal personnel  
 19           to run automated security monitoring;
- 20           c. Ordering that Defendant audit, test, and train its security personnel and employees  
 21           regarding any new or modified data security policies and procedures;
- 22           d. Ordering that Defendant provide employee training regarding the dangers and risks  
 23           inherent in using file-sharing websites;
- 24           e. Ordering that Defendant cease transmitting PII via file-sharing websites;
- 25           f. Ordering that Defendant cease storing PII on file-sharing websites;

- g. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for its provision of services;
- h. Ordering that Defendant conduct regular database scanning and security checks; and
- i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, personally identifiable information.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

- a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;
- b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, treble damages, attorneys' fees, expenses, costs, and such other and further relief as is just and proper;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;
- e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- f. An award of such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: February 27, 2023

**TOUSLEY BRAIN STEPHENS PLLC**

By: s/Kaleigh N. Boyd

Kaleigh N. Boyd, WSBA #52684  
Jason T. Dennett, WSBA #30686  
1200 Fifth Avenue, Suite 1700  
Seattle, WA 98101-3147  
Tel: (206) 682-5600  
Fax: (206) 682-2992  
kboyd@tousley.com  
jdennett@tousley.com

*Interim Liaison Counsel*

Bryan L. Bleichner\*  
Philip Krzeski\*  
**CHESTNUT CAMBRONNE PA**  
100 Washington Avenue South, Suite 1700  
Minneapolis, MN 55401  
Phone: (612) 339-7300  
Fax: (612) 336-2940  
bbleichner@chestnutcambronne.com  
pkrzeski@chestnutcambronne.com

John A. Yanchunis\*  
Ryan D. Maxey\*  
**MORGAN & MORGAN COMPLEX  
BUSINESS DIVISION**  
201 N. Franklin Street,  
7th Floor  
Tampa, Florida 33602  
(813) 223-5505  
jyanchunis@ForThePeople.com  
rmaxey@ForThePeople.com

*Interim Co-Lead Counsel*

1 Nathan D. Prosser\*  
2 **HELLMUTH & JOHNSON PLLC**  
3 8050 West 78th Street  
4 Edina, MN 55439  
5 Phone: (952) 522-4291  
6 nprosser@hjlawfirm.com

7 Terence R. Coates\*  
8 Dylan J. Gould\*  
9 **MARKOVITS, STOCK & DEMARCO, LLC**  
10 119 E. Court Street, Suite 530  
11 Cincinnati, OH 45202  
12 Tel: (513) 651-3700/Fax: (513) 665-0219  
13 tcoates@msdlegal.com  
14 dgould@msdlegal.com

15 Joseph M. Lyon\*  
16 **THE LYON FIRM**  
17 2754 Erie Ave.  
18 Cincinnati, OH 45208  
19 Phone: (513) 381-2333  
20 jlyon@thelyonfirm.com

21 Gary M. Klinger\*  
22 **MILBERG COLEMAN BRYSON PHILLIPS**  
23 **GROSSMAN, PLLC**  
24 221 West Monroe St., Suite 2100  
25 Chicago, IL 60606  
26 Telephone: (866) 252-0878  
gklinger@milberg.com

William B. Federman\*  
**FEDERMAN & SHERWOOD**  
10205 North Pennsylvania Avenue  
Oklahoma City, Oklahoma 73120  
Telephone: (405) 235-1560  
Facsimile: (405) 239-2112  
wbf@federmanlaw.com

A. Brooke Murphy\*  
**MURPHY LAW FIRM**  
4116 Will Rogers Pkwy, Suite 700  
Oklahoma City, OK 73108  
Telephone: (405) 389-4989

1 abm@murphylegalfirm.com

2 Samuel J. Strauss (WSB# 46971)  
3 **TURKE & STRAUSS LLP**  
4 613 Williamson Street, Suite 201  
5 Madison, WI 53703  
6 Phone: (608) 237-1775  
7 Fax: (608) 509-4423  
8 sam@turkestrauss.com

9 Carl v. Malmstrom\*  
10 **WOLF HALDENSTEIN ADLER FREEMAN &**  
11 **HERZ LLC**  
12 11 W. Jackson Street, Suite 1700  
13 Chicago, IL 60604  
14 Phone: (312) 984-0000  
15 malmstrom@whafh.com

16 Scott Edward Cole, Esq.\*  
17 Laura Van Note, Esq.\*  
18 Cody Alexander Bolce, Esq.\*  
19 **COLE & VAN NOTE**  
20 555 12th St., Ste. 1725  
21 Oakland, CA 94607  
22 Tel: (510) 891-9800  
23 Fax: (510) 891-7030  
24 sec@colevannote.com  
25 lvn@colevannote.com  
26 cab@colevannote.com

Mark J. Hilliard, Esq.  
**BROTHERS SMITH LLP**  
2033 N. Main St., Ste. 720  
Walnut Creek, CA 94596  
Tele: (925) 944-9700  
Fax: (925) 944-9701  
mhilliard@brotherssmithlaw.com

Bryan Paul Thompson  
Robert W. Harrer  
**CHICAGO CONSUMER LAW CENTER, P.C.**  
Cook County Firm No. 62709  
33 N. Dearborn St., Ste. 400  
Chicago, Illinois 60602  
Telephone: 312-858-3239



Fax: 312-610-5646  
Bryan.thompson@cclc-law.com

Michael Kind, Esq. (*Pro Hac Vice* Forthcoming)  
Nevada Bar No. 13903  
**KIND LAW**  
8860 South Maryland Parkway, Ste. 106  
Las Vegas, NV 89123  
Phone: (702) 337-2322  
Fax: (702) 329-5881  
Email: mk@kindlaw.com

Gary E Mason\*  
Danielle L. Perry\*  
Lisa A. White\*  
**MASON LLP**  
5101 Wisconsin Ave., NW, Ste. 305  
Washington, D.C. 20016  
Telephone: 202-429-2290  
gmason@masonllp.com  
dperry@masonllp.com  
lwhite@masonllp.com

Michael C. Subit  
**FRANK FREED SUBIT & THOMAS LLP**  
705 Second Ave., Ste. 1200  
Seattle, WA 98104  
Telephone: 206-624-6711  
msubit@frankfreed.com

\*admitted *pro hac vice*

*Additional Counsel for Plaintiffs*